## REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1, 3-5, 7, 9, 11 and 13-18 are pending in the present application. No claim amendments are presented, thus no new matter is added.

In the Office Action, Claims 1, 3-5, 7, 9 and 11-18 are rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. 6,248,946 to Dwek in view of U.S. Pub. 2001/0051996 to Cooper et al. (herein, Cooper).

Applicant respectfully traverses the above noted rejection under 35 U.S.C. § 103, as independent Claims 1, 9 and 13 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1, for example, recites, in part, a user authentication method for an authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

> ... transmitting, from said authentication server to said mobile information terminal, a certificate including a public key of the authentication server, an expiration date of the certificate and a digital signature;
>
> verifying an identity of the authentication server at the mobile information terminal based on the received certificate;
>
> generating, ***at a Web browser of the mobile information terminal, a secret key based on a result of the verification***;
>
> ***encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server***;
>
> transmitting the encrypted secret key from the mobile information terminal to the authentication server;
>
> receiving, at the authentication server from said mobile information terminal, the unique identification information as encrypted by said secret key at the Web browser installed on said mobile information terminal, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via a network ...

Independent Claims 9 and 13, while directed to alternative embodiments, recite similar features.

In rebutting the previously presented arguments regarding the above noted claimed features, the "Response to Arguments" section at pp. 2-4 cites various portions of Cooper, and asserts that this reference discloses the above noted claimed features. Applicant respectfully traverses the assertions set forth in the outstanding Office Action.

Particularly, p. 2 of the Office Action asserts that Cooper

> discloses the use of web browsers within mobile information terminals (par 38) whereby any and all necessary keys, digital certificates, and watermarks may be generated. Cooper describes in these portions how clients may use API and java applets running on their workstations to generate signed keys for existing certificates (pars 281-282 and 284). He also discloses that it is "contemplated by this application that each user device 115 will have some way to both store and manage digital certificates" (par 165) and how it is not unusual for any given user device 115 to have numerous digital certificates as it logs onto new website and performs other Web or Internet operations (par 164).

Applicant acknowledges that paragraphs [0164-0165] of Cooper do appear to describe that a user terminal 115 is capable of managing digital certificates used to access various websites. What Cooper fails to teach or suggest, however, is that the client workstation 115 verifies an identity of the authentication server at the mobile information terminal based on the received certificate, "generat[es], ***at a Web browser of the mobile information terminal, a secret key based on a result of the verification***", "***encrypts, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server***", and "transmits the encrypted secret key from the mobile information terminal to the authentication server", as recited in independent Claim 1.

More particularly, merely managing digital certificates at the user terminal 115 is no way analogous to performing the above noted claimed steps as a result of the verification of an identify of a server based on the received certificate.

Further, paragraphs [0281-282] of Cooper describe a process of distributing a digital certification from a Certificate Authority (CA) server 640 located at a content distribution system 200 to the user terminal 115. Paragraph [0284] of Cooper describes that a customer site 270 (e.g. including various servers 740, as shown in Fig. 7) may generate a signed key for an existing certificate received from the CA server 730 of the content distribution system 200. Based on this process, a new certificate may then be installed at the client workstation 115.

It is important to note that the customer site 200 is not the same as the user terminal 115. The customer site 270 includes various servers 740, as shown in Fig. 7, and installs the new certificate at the client workstation 115. Therefore, in the configuration described in paragraphs [0281-282] and [0284] of Cooper, the client workstation 115 is merely provided with a new certificate and does not generate any sort of signed keys to create the certificate.

Thus, paragraphs [0281-282] and [0284] of Cooper merely describe the processes implemented by a consumer site 270 to provide a digital certificate to a user workstation 115, and fail to teach or suggest the client workstation 115 verifies an identity of the authentication server at the mobile information terminal based on the received certificate, "generat[es], ***at a Web browser of the mobile information terminal, a secret key based on a result of the verification***", "***encrypts, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server***", and "transmits the encrypted secret key from the mobile information terminal to the authentication server", as recited in independent Claim 1.

Finally, the Office Action cites paragraphs [0289-0290] of Cooper. In referring to the client workstation 115, however, this cited portion of Cooper merely describes that the B2C server 740 interacts with a Java applet running on the client workstation 115 using the content distribution system 200 API functions. Cooper describes that this applet accepts

requests from the B2C server 740 using the content distribution system 200 API for installing and retrieving certificates.

Thus, this cited portion of Cooper again simply describes a process of installing and retrieving tickets at the client workstation 115, but fails to teach or suggest that the ticket is verified, that a secret key is generated based on the result of this verification, that a Web browser of the client workstation 115 encrypts the generated secret key using a public key of a server of the content distribution system 200, or that the client workstation 115 transmits the encrypted secret key from the client workstation 115 to the content distribution system 200.

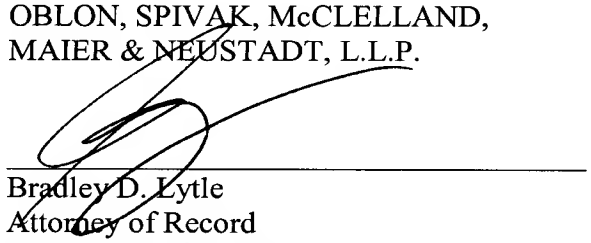
Moreover, Dwek fails to remedy the above noted deficiencies of Cooper. Therefore, Dwek and Cooper, even if combined, fail to teach or suggest a mobile information terminal that verifies an identity of the authentication server at the mobile information terminal based on the received certificate, "generat[es], ***at a Web browser of the mobile information terminal, a secret key based on a result of the verification***", "***encrypts, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server***", and "transmits the encrypted secret key from the mobile information terminal to the authentication server", as recited in independent Claim 1.

Accordingly, for at least the reasons discussed above, Applicant respectfully requests that the rejection of Claim 1 (and the claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn. For substantially similar reasons, it is also submitted that independent Claims 9 and 13 (and the claims that depend therefrom) patentably define over Dwek and Cooper.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3-5, 7, 9, 11 and 13-18 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)